



Utilizing CARVER to Determine the Relationship Between Your Assets & the Consequences of Threats

Presented by:

David Patterson, CPP, CFE, PSP, CHS

 **STEELE.**



What is CARVER

- Offensive target analysis tool
- Used by Army Special Forces for mission planning
- Based on a Commander's requirements/objectives
- Identifies the critical component of an asset that meets that requirement
- Recommended by USDA for food processing plant vulnerability assessments

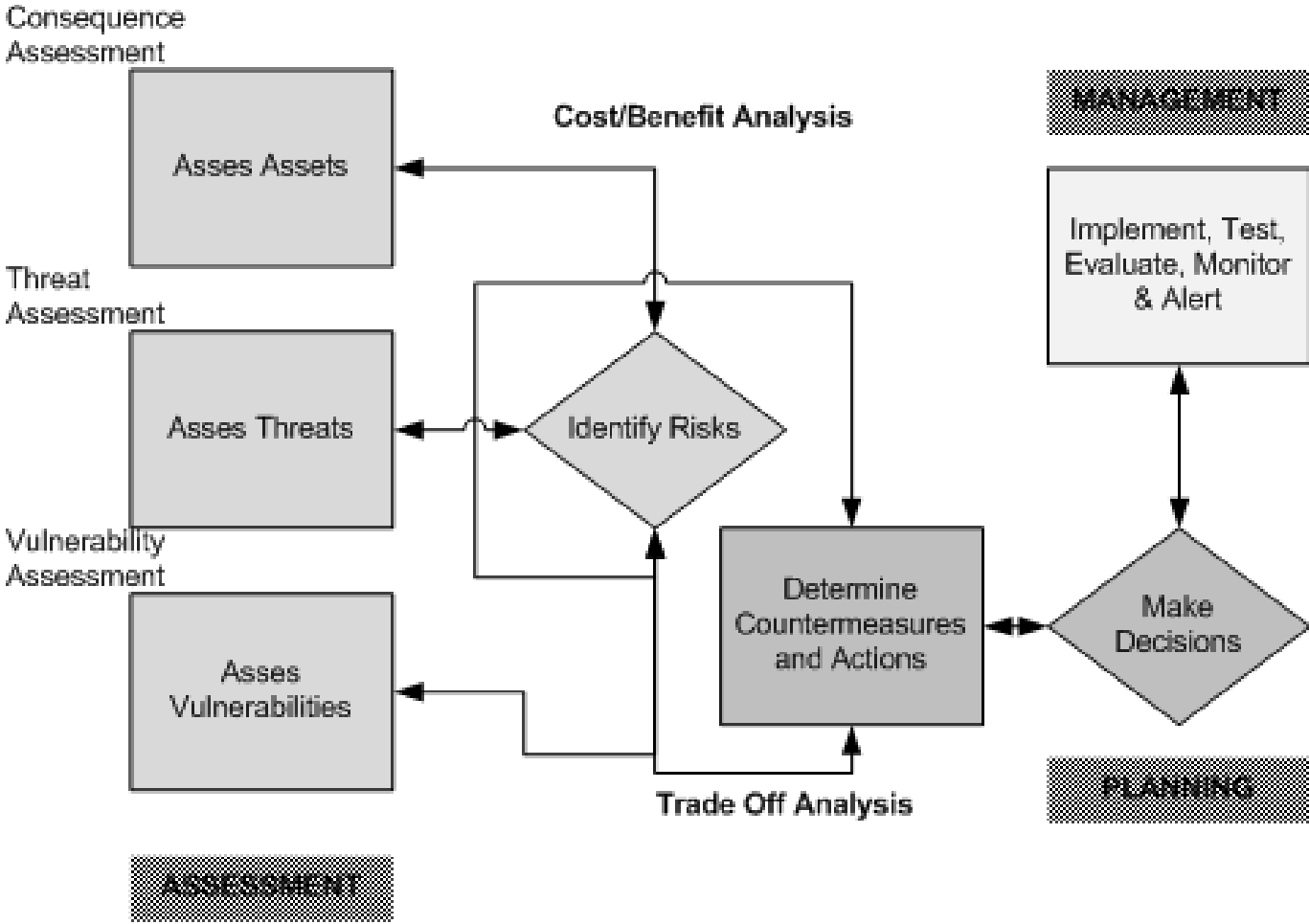


Knowledge Gained

- Understanding Characterizing Threats
- Understanding Design Basis Threat
- Understand Characterizing Assets
- Understand Vulnerabilities
- Understand Countermeasures
- Understanding the Resources and Limitations



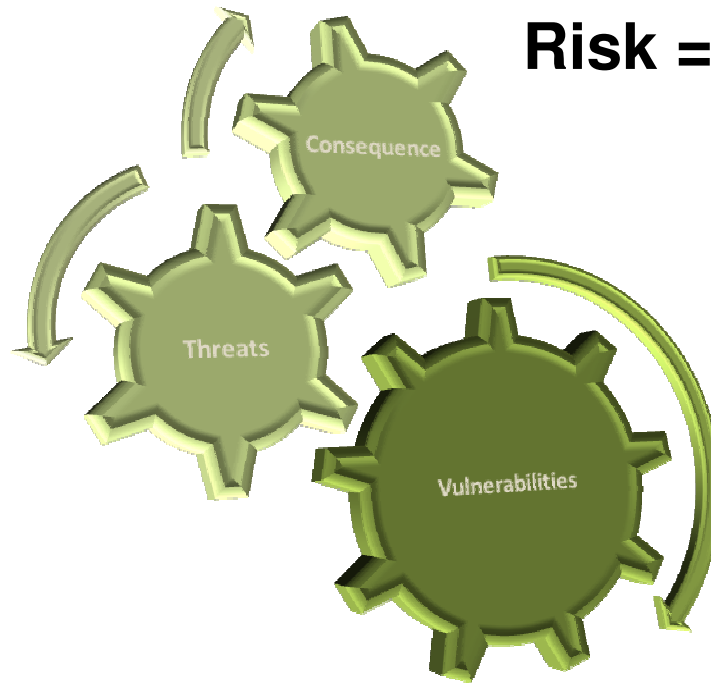
Risk Analysis Model





Calculating Risk

Risk



$$\text{Risk} = C(T*V)$$

Probability



Goal of the Risk Analysis

- Identify exploitable weaknesses
- Recommend actions to improve the protective posture



Vulnerability Assessment

- Identifies the weaknesses that allow a threat to be successful.
- Vulnerabilities
 - Physical
 - Operational
 - Information (non IT)
 - Cyber



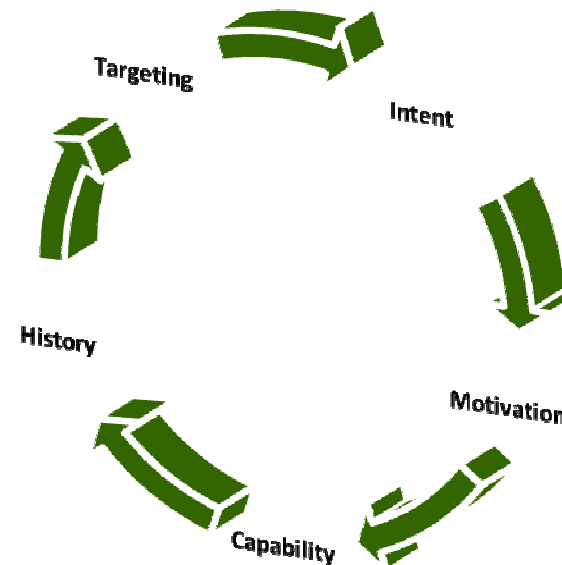
Threats

- Natural
 - Floods
 - Tornadoes
 - Hurricanes
 - Thunderstorms and Lightning
 - Winter Storms and Extreme Cold
 - Earthquakes
 - Volcanoes
 - Landslide and Debris Flow (mudslide)
 - Tsunamis
 - Wildfires
- Manmade
 - Crime
 - Terrorism
 - Unintentional Acts
 - Blackouts
 - Radiological Events
 - Hazardous Materials
 - Structure Fires
 - Chemical Spill
 - Transportation Accident



Threat Assessment

- **Threat Assessment** defines the level or degree of the threats.
- **Characteristics of threat**
 - Intent
 - Motivation
 - Capability
 - History of Action
 - Targeting





Design Basis Threat- DBT

- The threat forms the basis for the design of the protective system
- Threat must be defined in terms that are meaningful to the designer
 - Adversary tactics, tools, weapons and explosives
- Identify the adversary likely to threaten the asset, and
- The likelihood that they will attempt to compromise it



Adversaries

- Criminals - Unsophisticated, sophisticated, and organized crime
- Vandals/Activist
- Extremists
- Domestic Terrorists
- International Terrorists



Adversary- Tactics

- Unsophisticated Criminal may rely on low level forced entry limited to common hand tools
- Organized Crime high level of forced entry with unlimited hand and power tools and possibly limited explosives
- Domestic Terrorist may be capable of high level forced entry through stationary vehicle bomb
- International Terrorist may rely on all tactics



National Institute of Justice (NIJ) DBT Matrix

Type of Adversary	Number	Equipment	Vehicle	Weapon	Tactics
Terrorist outsider (may include an inside consultant)	2-3	Hand tools, power tools, body armor, chemical, biological agents.	4x4, all-terrain vehicles, pickup trucks, aircraft	Handguns, automatics, explosives	Cause catastrophic events, theft
Criminal	2-3	Hand tools, body armor	Foot, truck, aircraft	Handguns, explosives	Extortion, theft
Extremist	5-10	Signs, chains, locks, hand tools	Cars, buses	No weapons	Protest, civil disturbance, damage, destruction
Insider	1	Onsite equipment	Cars, pickup trucks, 4x4	Handguns, automatics, explosives	Destruction, violence, theft
Vandal	1-3	Paint	Cars, pickup trucks	Hunting rifles	Random shootings, tagging



Consequence

- Is an element of Risk that quantifies the loss to an asset.
- Consequence is characterized by the operational, economic, and health
- National Infrastructure Protection Plan (NIPP) four elements of consequence:
 - Economic
 - Health
 - Psychological
 - Governance



Assets

- People
 - Employees
 - Customers
 - Public
- Activities/Operations
 - Law Enforcement
 - Military
 - Proprietary activities
- Information
 - Classified
 - Public
 - IP
 - Sensitive
- Facilities
- Equipment/Materials
- Information Systems



Cost/Benefit & Trade Off Analysis

- **Cost Benefit Analysis** is part of the management decision process. Cost of protection compared to the cost of the asset.
- **Trade Off Analysis** refers to losing one quality or aspect of something in return for gaining another quality or aspect

A silver metal chain is positioned in the upper right corner of the slide, extending diagonally from the top edge towards the center. The background is a vibrant green with a subtle gradient and a curved, lighter green band that follows the path of the chain. The word "Countermeasures" is centered in the lower half of the slide in a bold, white, sans-serif font.

Countermeasures



Countermeasures

- A countermeasure is an action taken or a physical entity used principally to reduce or eliminate one or more vulnerabilities
- Countermeasures may affect the threat (intent and/or capability) as well as an assets value
- A countermeasure does not have to be elaborate to be effective



Defense in Depth

People	Process	Technology
Enhance employees awareness to thwart intelligence gathering	Consider national agency background checks on key personnel	Increase physical security of computer centers, implement access control
Incorporate security awareness training in on-going safety programs	Review contractor access to critical systems	Utilize monitors, sensors, and CCTV to replace manpower requirements
Train emergency response teams	Limit personal access to critical facilities	Improve computer security
Monitor employee training	Increase physical security at critical nodes	
	Increase intelligence and information interfaces	
	Sanitize information on web pages	
	Review and enforce operational procedures	



Security Functions

- **Deter**- countermeasures or actions prevent an adversary from taking an action
- **Detect**- countermeasures or actions identify a threat's existence, current activities, and or plans
 - Detect without an alarm, assessment, and communication is a deterrence
- **Delay**- countermeasures or actions slow down or delay actions. Physical security activities delay an adversary from entering a facility
 - A delay function before a detect function is primarily a deterrent
- **Deny**- countermeasures or actions prevent direct access
 - ***Devalue***
 - ***Respond***
 - ***Recover***

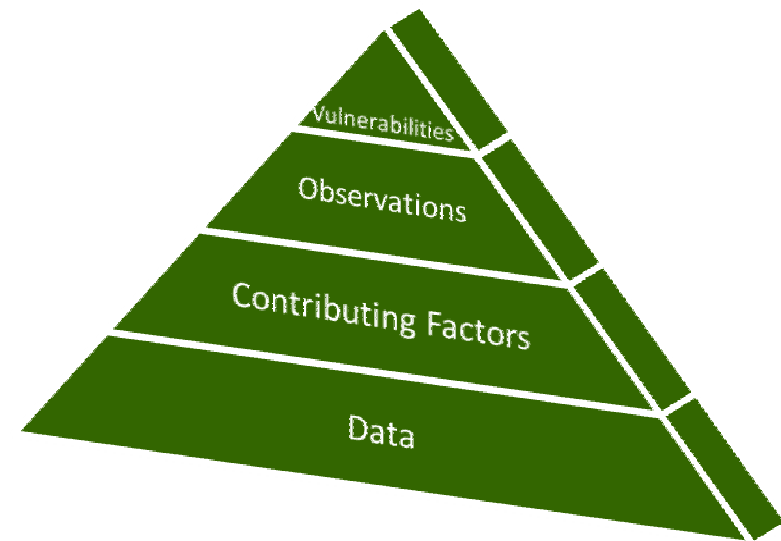


CARVER



CARVER

- Criticality
- Accessibility
- Recognizability
- Vulnerability
- Effect
- Recuperability





CARVER Methodology

- CARVER methodology assist in the analysis and examination of the interrelationships between assets, threats, vulnerabilities and countermeasures that protect a facility.
- CARVER is a unique analytical tool because it facilitates both a qualitative and a quantitative assessment of a facility's vulnerabilities based on offensive and defensive methodologies.



Criticality

- Criticality is target value to the threat
- A target is critical when its destruction or damage not only has a significant impact, but especially if the target meets the threat's objectives



Accessibility

- Can reach the target with sufficient personnel and equipment to accomplish its mission
- Accessible even if it requires the assistance of knowledgeable insiders
- Assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access
- The adversary must not only be able to reach the target but must also remain there for an extended period of time



Recognizability

- Recognizability is the degree to which it can be recognized by the adversary
- Weather has an obvious and significant impact on visibility, rain, snow, and ground fog may obscure observation
- Distance, light and season must also be considered



Vulnerability

- Vulnerable if the adversary has the means and expertise to successfully attack
- Scale of the critical component needs to be compared with the capability to destroy or damage it
- Existing countermeasures
- Attacking element may tend to:
 - Choose special components
 - Do permanent damage
 - Prevent or inhibit cannibalization
 - Maximize effects through the use of onsite materials
 - Cause the target to self-destruct



Effects

- Measure of possible economic, health, psychological, and governance impacts at the target and beyond
- Type and magnitude of given effects desired will help the adversary select targets and target components for attack
- Effect in this context addresses all significant effects, whether desired or not
- May be written as system effects



Recuperability

- Recuperability is measured in time:
 - That is, how long will it take to replace, repair, or bypass the destruction of or damage to the target?
- Recuperability varies with the sources and type of targeted components and the availability of spare parts availability



Selecting Countermeasures

- Utilize DBT for countermeasure design
- Select the countermeasures for further study that:
 - Provide the widest range of functions
 - Highest effectiveness
- Eliminate the weaker or bad ideas
- Use common sense when selecting countermeasures
- Understand the realities of the assessed organization

A silver metal chain is positioned in the upper right corner of the image, extending diagonally. The background is a vibrant green with a subtle gradient and a curved, lighter green line that sweeps across the upper portion of the frame. The text 'Case Study' is centered in the lower half of the image.

Case Study



Government Office Building

Case Center Building



Pointer 38°54'25.23" N 77°12'23.15" W

Streaming ||||| 100%

Eye alt 674 ft

© 2005 Google



General Information

- The subject of this threat and vulnerability assessment is an office complex consisting of 2 buildings located near Washington DC
- A Government office building is close by containing agency offices of Homeland Security.
- The East and West buildings house up to 28 tenants. Tenants range from Government Agencies (FDIC), Financial Institutions (Banks), Large Marketing Call Center, Health Laboratory, Information Technology (IT) Service Providers, Engineering, Consulting, and Training Providers
- Center is located near the conjunction of two major highways, across the street from a High School and a large housing complex, and next to a church.



Case Building



Fire Department



Public Safety



Image © 2005 Sanborn

© 2005 Google

Pointer 38°53'55.88" N 77°10'50.76" W

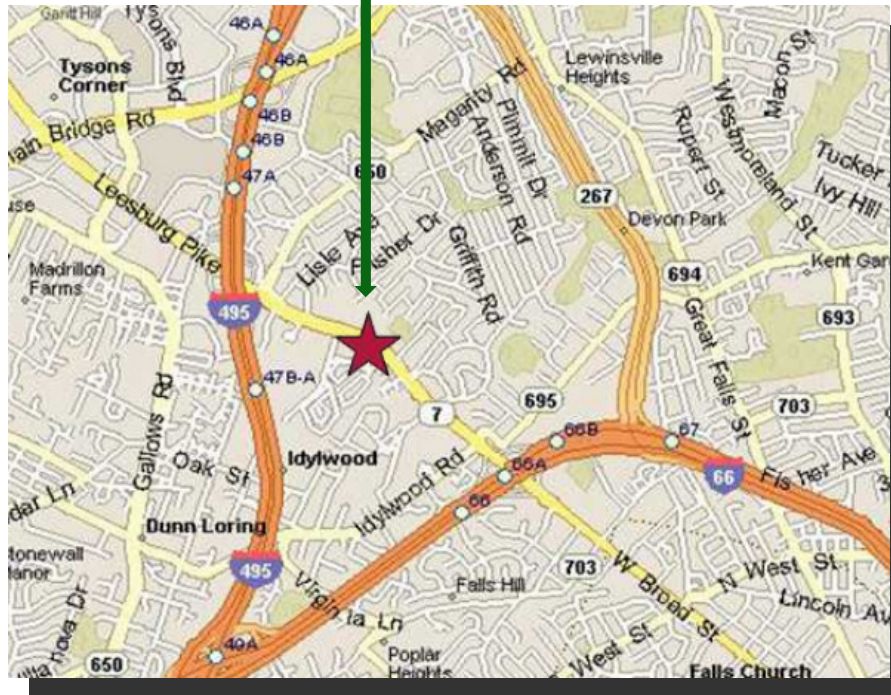
Streaming ||||| 100%

Eye alt 14723 ft



General Information (cont)

Case Center Location





Design Basis Threat Definition

One or more individuals gains undetected and unauthorized access to the facility with the intent to create a workplace violence incident.

Individuals are capable of defeating common security measures without hand or power tools.

May be armed with handguns or other weapons and may defend themselves if required.



Asset Characterization

Facility: Case Center											
Completed by:		Criticality									
Patterson											
CRITICAL ASSETS	West Building	East Building	Personnel	HVAC	Emergency Generator	Fuel Tank	Underground Parking Area	Intellectual Property	Server Site	Misc IT Hardware	TOTALS
West Building	2	4	2	2	3	1	5	4	3		26
East Building	4	4	2	2	3	1	5	4	3		28
Personnel	2	2	5	5	5	5	3	3	3		33
Building MEP Systems	4	4	1	3	3	4	2	2	2		25
Emergency Generator	4	4	1	3	3	4	2	2	2		25
Fuel Tank	3	3	1	3	3	4	2	2	2		23
Underground Parking Area	5	5	1	2	2	2	1	1	1		20
Intellectual Property	1	1	3	4	4	4	5	4	5		31
Server Site	2	2	3	4	4	4	5	2	4		30
Misc IT Hardware	3	3	3	4	4	4	5	1	2		29

CRITICALITY
 A target/asset is critical when its destruction or compromise will have significant impact on the output, mission or operation of the system or sub-system or component.

- 1 – Much Lower Than
- 2 – Lower Than
- 3 – The Same As
- 4 – Greater Than
- 5 – Much Greater Than



Asset Characterization

Facility: Case Center												
Patterson	Date:	Vulnerability										
CRITICAL ASSETS	West Building	East Building	Personnel	Bldg MEP Systems	Emergency Generator	Fuel Tank	Underground Parking Area	Intellectual Property	Server Site	Misc IT Hardware	TOTALS	
West Building	3	2	4	4	4	4	4	4	4	4	33	VULNERABILITY A system is vulnerable if the adversary has the means and the capability to carry out an attack against a system or asset. 1 – Much Lower Than 2 – Lower Than 3 – The Same As 4 – Greater Than 5 – Much Greater Than
East Building	3	2	4	4	4	4	4	4	4	4	33	
Personnel	4	4	5	5	5	5	5	5	5	5	43	
Bldg MEP Systems	2	2	1	3	2	3	4	4	4	4	25	
Emergency Generator	2	2	1	3	2	3	2	3	2	2	20	
Fuel Tank	2	2	1	4	4	4	5	4	4	4	30	
Underground Parking Area	2	2	1	3	3	2	4	4	4	4	25	
Intellectual Property	2	2	1	2	4	1	2	2	2	2	18	
Server Site	2	2	1	2	3	2	2	4	3	3	21	
Misc IT Hardware	2	2	1	2	4	2	2	4	3	3	22	



Threat Likelihood

Facility: Case Facility								
Date:	Likelihood							
Prepared By: D. Patterson								
Threats	Workplace Violence	Physical Destruction	Hazmat Release	Theft	Cyber	Vandalism	TOTAL	
Workplace Violence		5.00	5.00	4.00	5.00	3.00	22.00	1 - Much Lower Than 2 - Lower Than 3 - The Same As 4 - Greater Than 5 - Much Greater Than
Physical Destruction	1.00		4.00	1.00	3.00	1.00	10.00	
Hazmat Release	1.00	2.00		1.00	2.00	1.00	7.00	
Theft	2.00	5.00	5.00		4.00	2.00	18.00	
Cyber	1.00	3.00	4.00	2.00		2.00	12.00	
Vandalism	3.00	5.00	5.00	4.00	4.00		21.00	



Threat - Impact

Facility: CASE								
Date:				Impact				
Prepared By: STEELE				(Fill in DBT's across the top of row 4 to begin)				
DBT	Workplace Violence	Physical Destruction	Hazmat Release	Theft	Cyber	Vandalism	TOTAL	1 - Much Lower Than 2 - Lower Than 3 - The Same As 4 - Greater Than 5 - Much Greater Than
Workplace Violence		4.00	4.00	5.00	4.00	5.00	22.00	
Physical Destruction	2.00		5.00	4.00	4.00	4.00	19.00	
Hazmat Release	2.00	1.00		4.00	3.00	5.00	15.00	
Theft	1.00	2.00	2.00		2.00	4.00	11.00	
Cyber	2.00	2.00	3.00	4.00		5.00	16.00	
Vandalism	1.00	2.00	1.00	2.00	1.00		7.00	



Design Basis Threat

Facility: CASE FACILITY								
Date:	DESIGN BASIS THREAT							
Prepared By: D. Patterson								
THREATS	Workplace Violence	Physical Destruction	Hazmat Release	Theft	Cyber	Vandalism		
Likelihood	22	10	7	18	12	21		
Impact	22	17	17	12	15	7		
TOTAL	484	170	119	216	180	147		



CRITICAL ASSETS									
Date:									
Prepared By:									
CRITICAL ASSETS	DESCRIPTION	C - Criticality	A - Accessibility	R - Recovery	V - Vulnerability	E - Effect	R - Recognizability	RISK	
1	West Building	32	30	15	33	26	27	163	
2	East Building	34	30	15	33	28	29	169	
3	Personnel	45	41	45	43	43	37	254	
4	Building MEP Systems	18	19	31	25	18	22	133	
5	Emergency Generator	20	18	43	21	21	22	145	
6	Fuel Tank	15	34	21	29	19	22	140	
7	Underground Parking Area	15	23	25	25	19	22	129	
8	Intellectual Property	36	22	35	20	29	30	172	
9	Server Site	36	24	31	20	38	32	181	
10	Misc IT Hardware	19	29	9	21	29	27	134	



Vulnerability Assessment Methodology Application

- On-site review of all security measures
 - Architectural
 - Security Systems
 - Operations
- Facilitates the effective use of limited resources when prioritizing security upgrades
- Enables security specialists to identify which assets appear as targets
- Used globally to facilitate vulnerability assessments



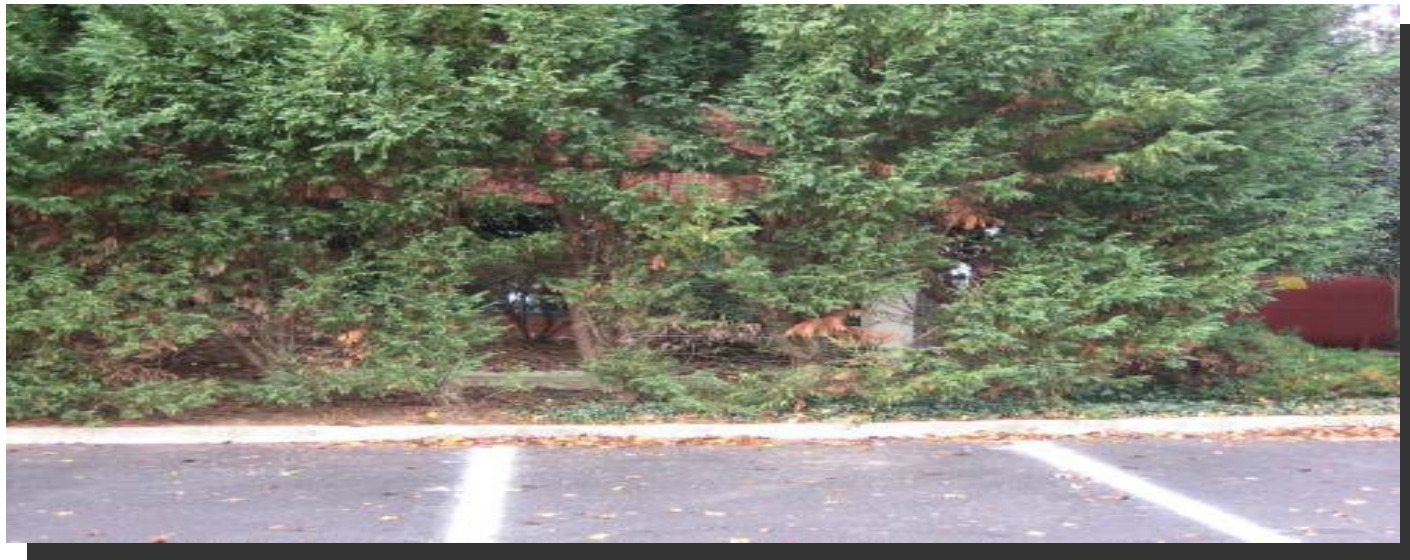
Bldg Exterior





Vegetation

- Vegetation allows intruders to hide





Emergency Power/Lighting Switch

- Emergency Power switch easily defeated





Emergency Generator Fuel

- Fuel Tank accessible





Exterior Lighting

- Inadequate





Faulty Mail Door Lock

- Unable to fully lock mailroom door





Garage Door

- Easily Defeated





Parking Lot Lighting

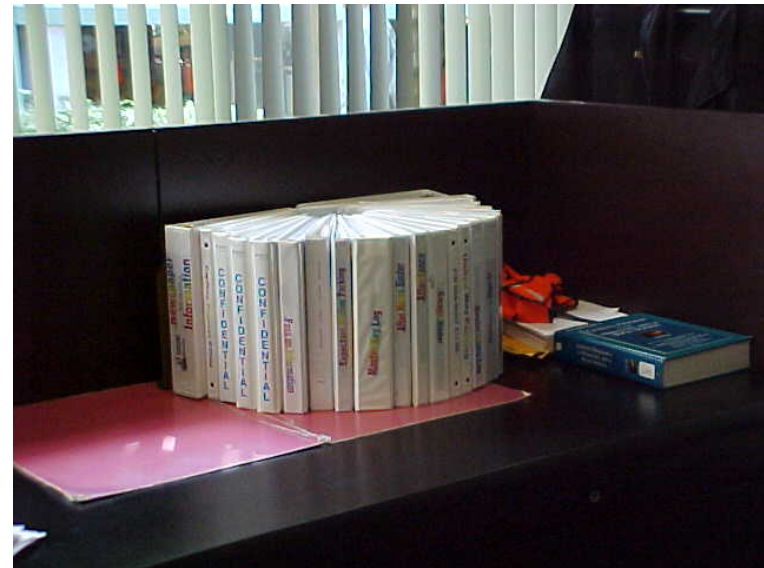
- Inadequate





Emergency Response

- No Response Plan
- No Emergency Response Team
- No Training
- No Exercises



Security Awareness

- **No Security Awareness Program**
- **No Training**
- **No Exercises**
- **No Incident Tracking**





Consequence Assessment

- **Injury or death to personnel due to:**
- **Inadequate lighting**
- **Lack of security cameras**
- **Improper garage doors and locks**
- **Lack of security alarm systems and other deterrence devices**
- **Disabling or destroying IT services due to vulnerabilities in emergency power system**
- **Lack of emergency response plan, organization, training, and exercises**
- **Lack of security awareness program, training, and exercises**



Risk Reduction Recommendations

- **Improve exterior lighting**
- **Install CCTV in garage area and building entrances**
- **Install access control system throughout bldg.**
- **Reduce vegetation**
- **Install panic alarms in parking lot**
- **Replace garage door**
- **Repair mail delivery door in East Bldg**
- **Harden emergency power system**
- **Implement emergency preparation and response plan and exercises**
- **Implement security awareness program and exercises**

A silver metal chain is positioned in the upper right corner of the image, extending diagonally towards the center. The background is a vibrant green with a subtle gradient and a curved white line that separates the chain from the rest of the page.

Q&A



Thank You

Greg Pearson
gpearson@wwsteele.com

David Patterson
dpatterson@wwsteele.com

 **STEELE.**